



## Security and the Avaya™ S8700 Media Server

Issue 1.2

May 2002

Converged Voice and  
Data Networks  
Customer Relationship  
Management  
Unified Communication  
Supported by:  
Avaya Labs and Services

**Communication without boundaries**



## **Table of Contents:**

<b>Section 1:</b>	Introduction
<b>Section 2:</b>	Elements of Security
<b>Section 3:</b>	Linux
<b>Section 4:</b>	Avaya S8700 Media Servers
<b>Section 5:</b>	Virus Protection
<b>Section 6:</b>	Testing
<b>Section 7:</b>	Environment



## Section 1: Introduction

This paper discusses security as it relates to an Avaya S8700<sup>1</sup> Media Server-based communication system. Its purpose is to inform owners and prospective owners of Avaya S8700 Media Servers of steps Avaya has taken to secure these systems and to provide information to assist owners in operating them in a secure manner. Because this information is valuable both to those who would like to protect the system and also to those who have more sinister motives, information is deliberately incomplete. So, for example, the ability to support one-time-passwords for user authentication is revealed, but not the mechanism of how this feature works.

Papers such as this that were written a few years ago would have focused mostly on toll fraud issues. Earlier systems did not interface with the data network and were neither susceptible to the types of attacks prevalent on those networks nor provided a gateway into such networks from which an attack might be launched. With the convergence of voice and data and the advent of IP Telephony, this is no longer true. Toll fraud is still an important issue, but one that is covered in other Avaya documentation. This paper focuses primarily on security issues, which arise due to the connection to the enterprise data network.

## Section 2: Elements of Security

A chain is only as strong as its weakest link, a house only as secure as its weakest door, window, or wall. If a burglar alarm is installed in a house but turned off, there are two consequences. One, the house is not secure and two, a lot of time, money,

and effort are wasted installing the alarm system in the first place. All doors, all windows, all walls, all systems (whether figurative or literal) must be secured.

Securing a system does not begin with the system itself, but with the people and organizations that operate or use it. One of the most important tools for securing a system is to have a written, published, security policy and to make sure it is enforced. RFC2196<sup>2</sup> will help you to create a security policy<sup>3</sup> and defines these steps:

1. Identify what you are trying to protect.
2. Determine what you are trying to protect it from.
3. Determine how likely the threats are.
4. Implement measures which will protect your assets in a cost-effective manner.
5. Review the process continuously and make improvements each time a weakness is found.

In examining whom to protect against, do not forget to look internally. A significant number of attacks come from within.

Part of the "measures" should include rules about behavior, the consequences of bad behavior, a path of escalation, and whom to notify of security issues. It does little good to enforce long randomized passwords if people are allowed to write the password on a sticky note on their computer monitors.

Often the weakest links are the most obvious and most easily overlooked and often involve human behavior. e.g., locking the doors to the equipment room and wiring closets. Denial of service is easier to accomplish with a hammer or wire cutters than with the root password.

<sup>1</sup> Though this paper the notation *Avaya S8700* Media Server is used when the discussion applies to either the Avaya S8700 Media Server - with MCC1 or SCC1 Media Gateway or Avaya S8700Media Server with G600 Media Gateway

<sup>2</sup> RFC's may be obtained on line from <http://www.ietf.org/home.html>

<sup>3</sup> See also RFC's 1244 and 1281and Telephone Systems Security, Air Force Systems Security Instruction 5033.



Security is always a trade-off; the more security, the more pain and the more cost. The more pain the more likely the human users will subvert the security measures. Make passwords too complex such that they are difficult to remember and people will write them down. Users prefer easy access without security; having to log on is inconvenient; not being able to cross mount file systems is inconvenient. However, everyone must endure some level of inconvenience if the system is going to be secure against those who would do harm. The security policy needs to define this level of pain and ensure that it is not circumvented by anyone.

### Section 3: Linux

The move from Oryx-Pecos<sup>1</sup> to open operating systems such as Linux or a version of Microsoft Windows® is often looked upon as a move to a less secure environment. To some extent this is true, but it is very important to understand why. Oryx-Pecos is used in systems, which either did not support data connectivity at all or supported such connectivity in interface cards isolated from the rest of the system. Without data connectivity or with very restricted connectivity, the types of security attacks are much reduced. Unfortunately, so is the functionality. Oryx-Pecos is more secure because it does not support the types of connectivity that the convergence of voice and data demand.

So why not enhance Oryx-Pecos? Aside from the economic reasons, there is a security paradox: *To make an operating system secure, reveal its inner most secrets.* When the operating system software is publicly available and used in varying environments and for a wide range of applications, there are many more eyes, both friend and foe, looking for security holes. The expertise of the entire technical community is brought to bear on the problem. The weakness created by exposing the flaws is outweighed by the probability that they will be fixed and the speed of getting it done.

Of the major operating systems (Unix, Linux, Windows), one is not *inherently* more secure than another. All are completely not secure out of the box. All can be made secure through the application of a good security policy, which includes proper administration and configuration, and diligent application of vendor updates when security problems are discovered. Linux has a slight advantage in that problems can be identified both by testing (hacking) and by review of the source code itself.

### Section 4: Avaya S8700 Media Servers

#### Linux

The Avaya S8700 Media Servers run under the Linux operating system. Linux has two important features, which are important for security. First, there is built in protection against certain types of Denial of Service (DOS) attacks such as SYN floods, ping floods, malformed packets, oversized packets, sequence number spoofing, ping/finger of death, etc. Attacks are recognized at the lower levels of the software and their effect blunted. (It is not possible for a target system to always provide service during a DOS attack; the protection is to automatically resume service as soon as the attack is removed.) Second, the Linux kernel is compiled with a set of options to precisely tailor its operation to maximize security consistent with required operation of the system. These include a number of built-in firewall and filtering options.

All file and directory permissions are set to minimize access as much as possible consistent with proper system operation. Multiple partitions exist on an Avaya S8700 Media Server disk drive. Each partition is restricted according to the type of data that it may contain. Some partitions contain only software executables; these partitions are mounted to allow program execution. Other partitions

<sup>1</sup> Oryx-Pecos is the proprietary operating system used by Avaya's DEFINITY® systems.



contain only data; execution of software from these partitions is disabled.

All unneeded services are disabled either permanently, or via administration for those services, which must be enabled in certain configurations. Disabled services and capabilities include NFS, SMB, X-windows, rcp, rsh, rlogin, and rexec. The System Administrator has additional control of which services are visible from the Ethernet interface connected to the enterprise LAN. (An Avaya S8700 Media Server has multiple Ethernet interfaces. More below.) Other Ethernet interfaces are permanently configured to limit services to those needed for proper operation.

#### **One-Time-Passwords**

Avaya MultiVantage™ Software, which powers the the Avaya S8700 Media Server, provides an option to use one-time-passwords for all logins. A *regular* password account uses a fixed user name (ID) and a password, which can be used multiple times to log into the system. A person who can monitor (network sniffer) the login messages can capture this password and use it to gain access. A *one-time-password* uses a fixed user name, but not a fixed password. Instead, every time a user attempts to log in, they must supply a password, which is unique to that session and which will be incorrect if used again. Even if the password is compromised, it cannot be re-used immediately or at a later time, even by the same person from the same terminal. One-time-passwords can be enabled for each login on an Avaya S8700 Media Server.

#### **Shell Access**

Access to a "shell" from which arbitrary commands may be executed is not granted by default to a login on an Avaya S8700 Media Server. When a login is created, the system administrator can specify whether or not the account is permitted to have shell access. Accounts, which are denied shell access, receive either an Avaya MultiVantage

Software administration screen or a WEB page upon successful login. In both cases, the operations that may be performed are restricted. In general, only individuals that perform hardware or software maintenance of the server need shell access.

#### **Root Access**

On a Linux system the highest level of administrative access is known as "root". Direct login to a root level account is not permitted on an Avaya S8700 Media Server. Administrative access, which requires root level permissions, is handled via "proxy" programs, which grant specific access to specific accounts. The ability to obtain full root level access is granted only in very special circumstances.

#### **Remote Access**

Each Avaya S8700 Media Server is configured with a modem to support remote maintenance access and origination of maintenance alarms calls. The server logins, which are used to establish this remote connection, are separate from those that allow administrative functions. One account is used to establish a connection; once the link is established, a second login is required using a separate account.

Use of the dial in line can be restricted for incoming calls by choosing one of the following:

- disallow all incoming calls
- allow one incoming call only
- allow all incoming calls

When the interface is set to "allow one incoming call only", the line is enabled to answer a single call. As soon as a call arrives, the line is disabled and must be re-enabled via administration before another call will be accepted. This feature does not inhibit outgoing alarm calls, which are needed for maintenance. The feature is intended to be used as follows. Normally, the line is disabled for all calls. When a maintenance activity is needed, the



maintenance technician must contact the server administrator via telephone, e-mail, etc. and request the line be activated. The server administrator must then log in to the server and enable the line for one call only. The maintenance technician then calls the server, performs necessary maintenance and disconnects. At this point the line is automatically disabled again.

Enabling the data line for one call only is a good example of a feature that illustrates the trade-off required between security and convenience. Having the data line disabled provides better security. But during diagnostic activity when multiple calls must be made, the server administrator must be called to manually re-enable the line for each call. This can be a nuisance and slow down the maintenance work. In addition, Avaya employs *expert systems* technology to contact systems automatically for monitoring and diagnostics. Disabling the data line disables this technology, resulting in higher maintenance costs and possibly longer down times when a failure does occur.

### **Secure Access**

Typical mechanisms of server access include *telnet*, *WEB Browser (HTTP)*, and *FTP* for file transfers. Each of these mechanisms can support login authentication, but suffer a common weakness. During the login sequence, the password being supplied by the user is sent in clear text. This allows a person with a network monitor/sniffer to capture the password and gain access. In addition these mechanisms transmit all the session information in clear text. Some of this information might contain data such as account codes, authorization codes or other data useful to an attacker. To overcome these problems, Avaya S8700 Media Servers also support *Secure Shell Access (SSH)*, *Secure Copy (SCP)*, and secure WEB access using the *Secure Sockets Layer (SSL) with HTTPS*.

SSH and SCP provide an access mechanism for terminal access and file copy that encrypt the entire

session including the login sequence as well as subsequent data transfer.

SSL/HTTPS provide a similar mechanism for WEB access. All WEB access to an Avaya S8700 Media Server is via a secure connection. Unencrypted WEB access is not supported. In addition, the Avaya S8700 Media Servers support one-time-passwords for logins through these mechanisms even though the exchange is already encrypted.

On an Avaya S8700 Media Server, the FTP service is disabled by default. Each time a file is to be transferred to the server, an administrator must log in and enable the FTP server. The file is then transferred using *anonymous* FTP, and the FTP server can then be disabled. Using anonymous FTP in this manner avoids the problem of sending passwords in clear text. However, SCP is the preferred method of transferring files.

### **Monitoring and Alarming**

Avaya S8700 Media Servers support a variety of security monitoring features. Sessions are automatically disconnected after a period of inactivity. Accounts are automatically locked out for a period of time as a consequence of consecutive failed login attempts. Files and directories are monitored and audited by *tripwire*. All login sessions, whether successful or not, are logged. All user activity is logged. Security events are alarmable events, which are reported in two ways. A maintenance alarm is called out to an Avaya Maintenance center via an analog telephone call. An SNMP trap can be sent to one or more destinations.

### **Data Protection**

Attacks against a system are not limited to attempts to find holes in the access structure. There is also a technique known as *data mining* or *dumpster diving* that can be used even more effectively if the system owner is not careful.



Avaya S8700 Media Servers have the ability to store (backup) copies of critical configuration information including authentication and account information on external systems. If this information is stored in clear text, and the file server on which it is stored is compromised, the Avaya S8700 Media Server could be compromised. To make this more difficult, Avaya S8700 Media Servers have the ability to encrypt all backup data. This option should always be used when using the backup feature. It is the user's responsibility to remember the key, because Avaya will not be able to assist if the key is forgotten.

From time to time, new software features are created which require that the software or firmware be updated. This process involves the transfer of executable files to the Avaya S8700 Media Servers or other system components from a variety of

sources. It is important that these files arrive exactly as they were created at Avaya. To prevent malicious modification in transit, all distributions are cryptographically signed so that modifications can be detected and installation aborted.

### LAN Isolation

An Avaya S8700 Media Server based system contains multiple Ethernet Network Interfaces (NICs).

- Each Avaya S8700 Media Server with Avaya MCC1 or SCC1 Media Gateway contains 5 Ethernet interfaces (NICs). Each NIC is dedicated to a specific function or functions.
- Port networks, which contain the interfaces to which telephone devices connect, contain additional Ethernet interfaces.

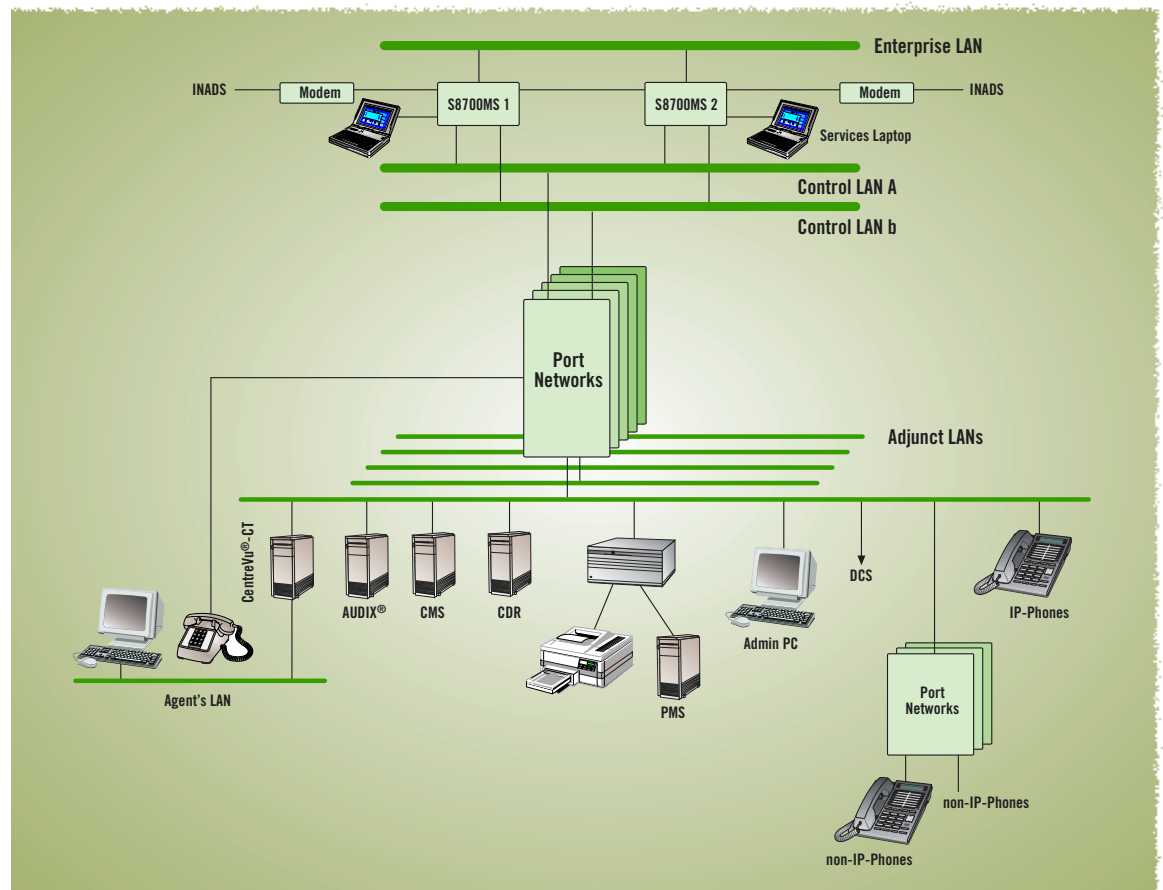


Figure 1. Avaya S8700 Media Server with Avaya MCC1 or SCC1 Media Gateway LANs



Figure 1 illustrates the different LANs, which are possible on an Avaya S8700 Media Server with Avaya MCC1 or SCC1 Media Gateways system along with some of the common adjuncts that might connect to these LANs.

The enterprise LAN, adjunct LANs and agent's LAN, can all be connected together to form one network, or they can be kept physically separate for either traffic or security reasons. In order to provide the most secure environment possible for the system, network access should be divided into separate zones of control (sometimes referred to as DMZs). Figure 1 illustrates one such configuration. One VLAN could be administered for administrative traffic, one for call signaling, another for voice bearer traffic, etc. Layer 3 boundary devices (routers, layer 3 switches, and firewalls) should be administered to enforce the corporate security policy on traffic destined for the Avaya S8700

Media Server, its Avaya MCC1 or SCC1 Media Gateways, or adjuncts. Packet filters could be put in place to permit administrative access only from an administrator's PC and to deny access from the Avaya S8700 Media Server or its gateways to the corporate LAN while allowing call signaling and bearer traffic from all IP telephones appropriate access. Figure 2 illustrates this possibility.

The Avaya MultiVantage Software can be configured to allow only certain types of access to specific LAN interfaces on its port networks. So, for example, in figure 2, even if one were to connect an administration terminal to one of the other LANs, administration access would be denied.

The 5 Ethernet interfaces (NICs) used by the Avaya S8700 Media Servers with Avaya MCC1 or SCC1 Media Gateways are already dedicated to specific functions. The two control LANs are only used to

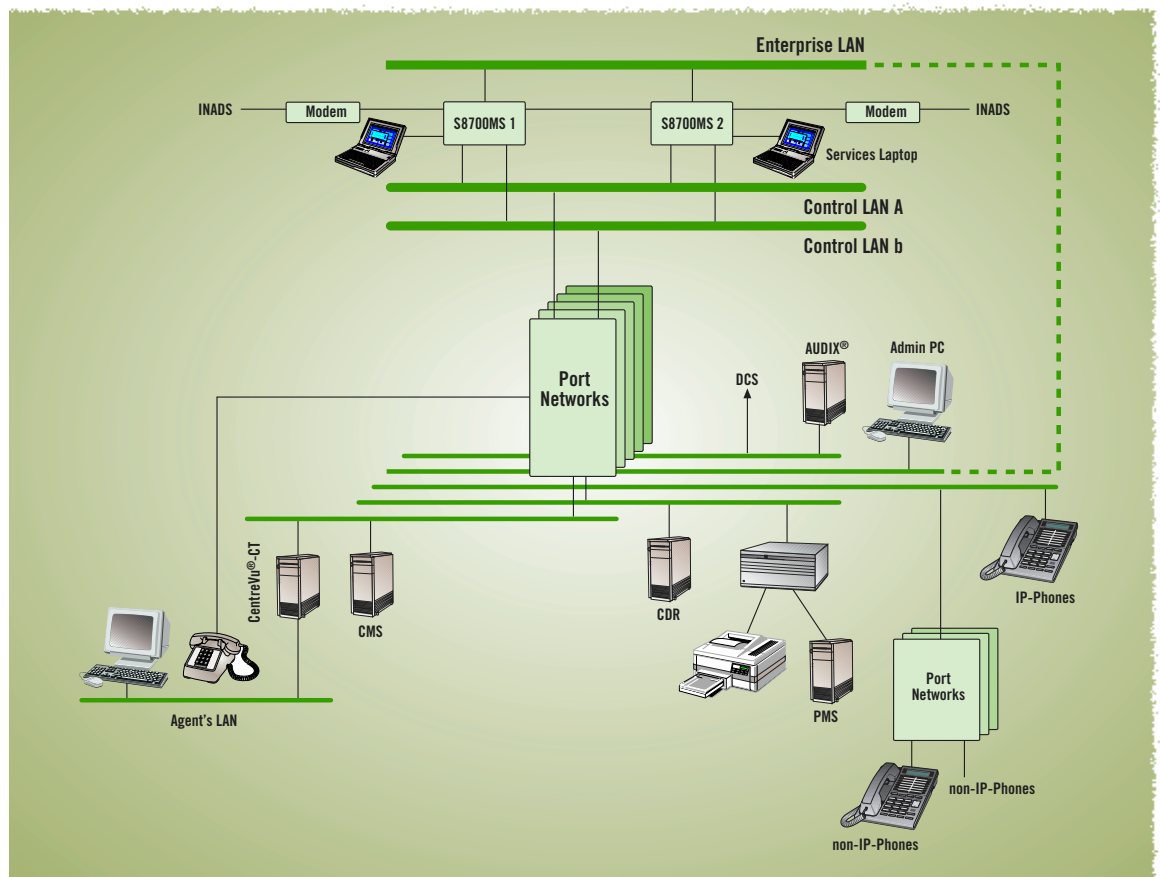


Figure 2. Isolated LANs (Avaya S8700 Media Server with MCC1 or SCC1 Media Gateways)



connect between the servers and the port networks. These two LANs must be private LANs and carry no other traffic. The duplication interface is a point-to-point LAN that is only used to send information between the two servers. The laptop interface is a point-to-point LAN that is used only for local administration and carries no other type of traffic. The enterprise LAN is used for administration and time synchronization; telephony traffic does not use this LAN. However, in this case, it is possible to subvert this security measure by interconnecting the enterprise LAN NIC with one of the other LANs shown.

The Avaya S8700 Media Servers with Avaya G600 Media Gateways also have five NICs each, but these interfaces are used differently from the Avaya S8700 Media Server with Avaya MCC1 or SCC1 Media Gateways. On an Avaya S8700 Media Server with Avaya G600 Media Gateways, the enterprise LAN and Control LANs are connected together, there is only one control LAN, and there are two spare NICs that are not used. Figure 3 illustrates this configuration. The messages between the Avaya S8700 Media Server and the Avaya G600 Media Gateways are encrypted. This feature is not available on the Avaya S8700 Media Server with Avaya MCC1 or SCC1 Media Gateway, and so the control LANs must be connected as private LANs.

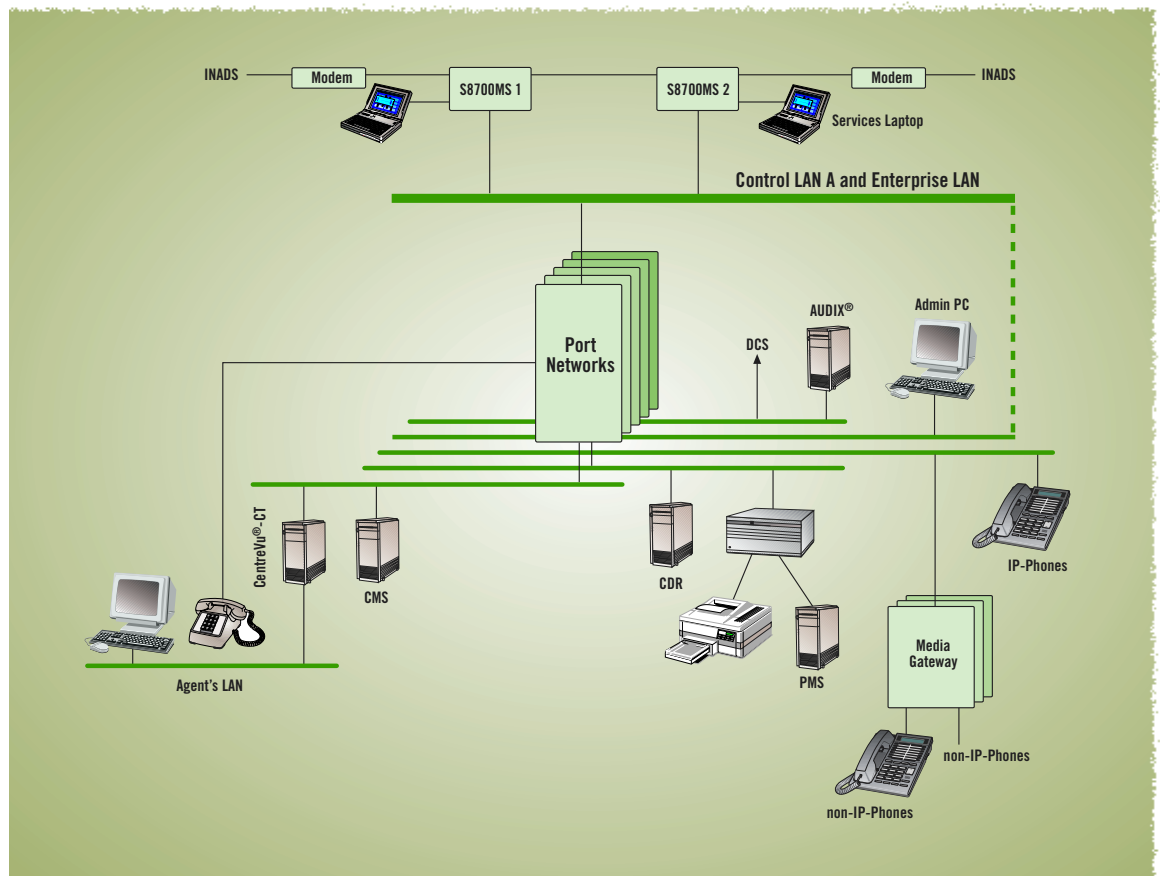


Figure 3. Isolated LANs  
(Avaya S8700 Media Server  
with G600 Media Gateway)



## Section 5: Virus Protection

The viruses and worms that have made the headlines have mostly targeted Microsoft Windows operating systems or more specifically some of the Microsoft application software such as IIS, Exchange, Outlook, or Word. Because the Avaya S8700 Media Server is Linux-based and does not employ any of this software, it has some level of natural immunity. In addition, viruses and worms are most commonly delivered via e-mail, by visiting infected WEB sites, or by sharing of disk drives. The Avaya S8700 Media Server does not support incoming e-mail, does not support forwarding of e-mail (since there is no incoming e-mail in the first place), does not contain a WEB browser, and does not support NFS or SMB (i.e. does not share drives). All file transfers to the Avaya S8700 Media Server are restricted and are cryptographically signed to prevent introduction of unwanted software.

In addition to this natural immunity, the Avaya S8700 Media Server incorporates additional anti-tampering features. The disk drive is divided into multiple partitions. Executable code is stored in separate partitions from data; data are likewise stored in separate partitions, which do not have execute permissions. Direct root level access is not normally permitted, and when it is granted, the login is protected by one-time-passwords. This is important because one of the first goals of an attacker is to obtain root level access as this provides the opportunity for the most destruction. Login accounts on the Avaya S8700 system do not necessarily receive any type of shell access. This is also important because shell access allows the user to enter commands at will whereas the more controlled access limits the user to the functionality presented on menus or screens. The files and file system is monitored by *tripwire*. This software product maintains a cryptographically encoded signature of the files on the system and generates alarms in the event any unexpected changes occur.

The Avaya S8700 Media Server development team considered adding some form of virus scanning software to its repertoire. However, virus scanner software for Linux is not common, generally because the market and threat is not sufficiently large to entice scanner vendors. In addition, those vendors that do offer Linux scanners primarily scan e-mail to prevent the spread of a virus to Windows based machines on the same network; they do nothing for the Linux box itself. As already stated, Avaya S8700 Media Server has no incoming e-mail and so there is nothing for these products to scan.

## Section 6: Testing

During the development of the Avaya S8700 Media Server based system or in production of upgrades to its software, Avaya subjects the system to a variety of common "attack tools" to find any overlooked or accidentally created security holes. The exact set of tools, which are used, varies to keep up with the technology. Common tools include nmap and nessus. Security problems found by these efforts are corrected prior to the product or update being released.

## Section 7: Environment

Avaya has taken steps to make the Avaya S8700 Media Servers as secure as is reasonable; consistent with the operational needs of the product and business it serves. Security, however, does not end with the servers. These servers will be connected to one or more networks, which are in turn connected to other equipment in the enterprise. As a minimum, these servers should be located behind a firewall. Where this firewall is located with respect to other LAN components must be designed on a case-by-case. Avaya professional services can assist owners in configuring their networks for both security and optimal Voice over IP (VoIP) operation.

In addition other vendors specialize in this type of consulting. Owners are advised to seek assistance if internal staff is not trained in these areas. Security holes which arise from negligence, ignorance, or oversight or the pressures of schedule or budget are all equally usable by those who would do harm.

Malicious activity is a moving target. What is safe today may not be safe tomorrow. Avaya is committed to providing appropriate secure solutions for its products and continuously monitors the nature of these threats. As this paper is written, the Avaya S8700 Media Servers are appropriately secure against the known threats. Avaya will respond quickly should new threats appear. Your Avaya account team and Avaya's support web site (<http://www.avaya.com/support>) should be consulted for the latest information in this area.

The Avaya logo is rendered in a bold, red, sans-serif font. The letters are closely spaced, and the 'A' at the end has a distinctive shape with a small gap at the top.